STATE OF ALABAMA

Information Technology Standard

Standard 670-04S1_Rev A: Virus Protection

1. INTRODUCTION:

Viruses can infect IT systems by a wide variety of methods including email messages, the Internet and through accessing infecting files on USB drives, floppy disks, and CDs. Viruses can propagate very quickly as they are easily spread to other network-connected PCs. It is vitally important that all IT systems have anti-virus software installed, current, and running to provide real-time protection to the State's network infrastructure and data.

2. OBJECTIVE:

Establish statewide virus and malware protection requirements to safeguard State of Alabama networks, IT components, and data from viruses and other malicious logic.

3. SCOPE:

These requirements apply to all administrators and managers of State-managed information system resources. These requirements address the prevention of malicious logic (viruses, worms, and other self-replicating malware); malicious code incident handling is covered in State IT Procedure 600-04P2: Incident Handling.

4. REQUIREMENTS:

Anti-virus (AV) software shall be acquired, configured, and used in accordance with the following requirements.

4.1 ANTI-VIRUS PRODUCT SELECTION

Use only licensed (in accordance with State software licensing and use policy) anti-virus products that are ICSA certified. ICSA Labs is the security industry's central anti-virus product testing and certification facility. View the latest list of ICSA-certified anti-virus products at http://www.icsalabs.com.

AV programs shall provide for centralized virus pattern updates, alerting, compliance reporting, and automatic cleanup and repair.

4.2 ANTI-VIRUS SOFTWARE CONFIGURATION

Every machine shall have an AV program installed and active for on-access and on-demand virus detection.

Ensure the anti-virus software installation is a supported version.

Ensure the site has a formal migration plan for removing or upgrading anti-virus software prior to the date the vendor drops security patch support.

Ensure the latest maintenance rollup or software update for the anti-virus software is applied.

Ensure AV software installation and update files are only downloaded from a trusted site or directly from the vendor.

Ensure AV definition/signature files are automatically updated at least weekly. It is recommended the signatures be updated daily, subject to availability.

Ensure standard procedures exist and are executed for updating AV definition/signature files on isolated networks or standalone systems at least weekly.

Ensure signature files are no older than 14 days. In the event that the AV vendor does not release a signature file in the last 14-day period, then the most current release is required.

Do not use Beta or non-production versions of definition/signature files on production machines.

Configure AV software to start on-access protection automatically when the operating system is booted.

Configure AV software to perform a virus scan of the local hard drives at least weekly. Scanning at boot time (or daily) is recommended when this would not cause a significant impact to operations.

At a minimum, AV software shall be configured to scan the following file types in all directories except those used to hold files quarantined by the anti-virus software:

- Executable, service, and driver files (i.e., files suffixed with .bat, .bin, .com, .dll, .exe, .sys, etc.)
- Application data files that could contain a form of mobile code (i.e., files suffixed with .doc, .dot, .rtf, .xls, .xlt, .hta, .wsh, scrap objects, etc.)

Configure AV software to scan files incoming from floppy disks, e-mail attachments, web site downloads, and any other locally attached devices such as Zip Drives, USB Drives, or Personal Digital Assistants.

Ensure the AV software, when running in on-access mode, is configured to inform the user, and have a mechanism to notify the SA at the time a virus is detected. Report virus or malware infections in accordance with incident reporting procedures.

Configure systems to prevent users from disabling AV software updates and virus scans. Virus definition updates and virus scans shall not be stopped or disabled except by domain administrators.

Maintain AV log files for at least 30 days.

4.3 REMOTE ACCESS DEVICES

Ensure that all remote workstations and servers used by State employees, contractors, and third-party entities that access internal networks are protected with virus-scanning software equivalent to that used by the State for network-attached devices.

4.4 EMAIL SYSTEMS

Email servers shall provide additional virus protection to prevent malware from entering the network. In addition to standard system virus-scanning, email and proxy servers will additionally scan all incoming email (including attachments) for the existence of viruses or malicious code before it is accepted by the system and before it leaves the system. Infected messages shall be dropped.

4.4.1 Prohibited Attachment Files Types

Attachments of certain types of files can contain active content that may be used to spread malware, therefore, attachments of the following file types are prohibited.

Table 4-1: Prohibited Attachment File Types

EXTENSION	PROGRAM or EXTENSION FUNCTION
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.app	Microsoft FoxPro application
.asp	Active server pages
.asx	Advanced stream redirector file
.bas	BASIC source code
.bat	Batch file
.cer	Internet security certificate file
.chm	Compiled HTML help file
.cmd	Windows NT command file
.cnf	Configuration File
.com	Command file program
.cpl	Control panel extension
.crt	Certificate file
.csh	Unix shell script (among others)
.dll	Dynamic link library
.exe	Binary executable program
.fxp	Microsoft FoxPro compiled source
.gadget	Windows Vista gadget
.hlp	Help file
.hta	Hypertext Application
.inf	Information or Setup file
.ins	Internet naming service (IIS)
.isp	Internet communication settings (IIS)
.its	Internet Document Set
.js	JavaScript file
.jse	JavaScript encoded file
.ksh	Unix shell file
.lnk	Windows shortcut file
.mad	Microsoft Access Module Shortcut
.maf	Microsoft Access File
.mag	Microsoft Access Diagram Shortcut
.mam	Microsoft Access Macro Shortcut
.maq	Microsoft Access Query Shortcut
.mar	Microsoft Access Report Shortcut

EXTENSION	PROGRAM or EXTENSION FUNCTION
.mas	Microsoft Access Stored Procedure
.mat	Microsoft Access Table Shortcut
.mau	Microsoft Access Shortcut
.mav	Microsoft Access View Shortcut
.maw	Microsoft Access Data Access Page
.mda	Microsoft Access add-in program
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.mdt	Microsoft Access file
.mdw	Microsoft Access file
.mdz	Microsoft Access wizard program
.mhtml	Archived Web Page
.msc	Microsoft Common Console document
.msi	Windows installer file
.msp	Windows Installer patch
.mst	Windows SDK setup transform script
.ops	Office profile settings file
.pcd	Microsoft Visual Test
.pif	Windows program information file
.prf	Windows system file
.prg	Program file
.pst	Microsoft Outlook Personal Folder File
.reg	Registry data file
.scf	Windows Explorer Command file
.scr	Screen saver
.sct	Windows® script component
.shb	Document shortcut
.shs	Shell scrap object file
.tmp	Temporary File/Folder
.url	Internet address
.vb	VBScript file; Visual Basic source file
.vbe	VBScript encoded script file
.vbs	VBScript file; Visual Basic for applications script
.vsmacros	Visual Studio .NET Binary-based Macro Project
.vss	Visio stencil
.vst	Visio template
.vsw	Visio workspace
.ws	Windows Script File
.wsc	Windows script component
.wsf	Windows script file
.wsh	Windows script host settings file
.xsl	XML style sheet

4.4.2 Handling Attachments

The handling of prohibited file type attachments shall be specified in operational procedures.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 670-04: Virus Protection

6.2 RELATED DOCUMENTS

Information Technology Policy 630-06: Software Licensing and Use

Information Technology Standard 680-01S3: Removable Storage Devices

Information Technology Procedure 600-04P1: Incident Reporting

Information Technology Procedure 600-04P2: Incident Handling

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	3/22/2007	
Rev A	4/17/2008	Completely revised. Significant change: reduced scan requirement from daily to weekly; daily scans are recommended.